Quantum Cryptography Protocol

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to the field of quantum cryptography, and more particularly to a method for exchanging a key with guaranteed security using systems vulnerable to photon number splitting (PNS) attacks, i.e. a quantum cryptography protocol robust against PNS attacks.

2. Discussion of Prior Art

If two users possess shared random secret information (below the "key"), they can achieve, with provable security, two of the goals of cryptography: 1) making their messages unintelligible to an eavesdropper and 2) distinguishing legitimate messages from forged or altered ones. A one-time pad cryptographic algorithm achieves the first goal, while Wegman-Carter authentication achieves the second one. Unfortunately both of these cryptographic schemes consume key material and render it unfit for use. It is thus necessary for the two parties wishing to protect the messages they exchange with either or both of these cryptographic techniques to devise a way to exchange fresh key material. The first possibility is for one party to generate the key and to inscribe it on a physical medium (disc, cd-rom, rom) before passing it to the second party. The problem with this approach is that the security of the key depends on the fact that it has been protected during its entire lifetime, from its generation to its use, until it is finally discarded. In addition, it is very unpractical and tedious.

Because of these difficulties, in many applications one resorts instead to purely mathematical methods allowing two parties to agree on a shared secret over an insecure communication channel. Unfortunately, all such mathematical methods for key agreement rest upon unproven assumptions, such as the difficulty of factoring large integers. Their security is thus only conditional and questionable. Future mathematical developments may prove them totally insecure.

Quantum cryptography (QC) is the only method allowing the distribution of a secret key between two distant parties, the emitter and the receiver, [1] with a provable absolute security. Both parties encode the key on elementary quantum systems, such as photons, which they exchange over a quantum channel, such as an optical fiber. The security of this method comes from the well-known fact that the measurement of an unknown quantum state modifies the state itself: a spy eavesdropping on the quantum channel cannot get information on the key without introducing errors in the key exchanged between the emitter and the receiver. In equivalent terms, QC is secure because of the no-cloning theorem of quantum mechanics: a spy cannot duplicate the transmitted quantum system and forward a perfect copy to the receiver.

Several QC protocols exist. These protocols describe how the bit values are encoded on quantum states and how the emitter and the receiver cooperate to produce a secret key. The most commonly used of these protocols, which was also the first one to be invented, is known as the Bennett – Brassard 84 protocol (BB84) [2]. The emitter encodes each bit on a two-level quantum system either as an eigenstate of σ_x ($|+x\rangle$ coding for "0" and $|-x\rangle$ coding for "1") or as an eigenstate of σ_y ($|+y\rangle$ or $|-y\rangle$, with the same convention). The quantum system is sent to the receiver, who measures either σ_x or σ_y. After the exchange of a large number of quantum systems, the emitter and the receiver perform a procedure called basis reconciliation. The emitter announces to the receiver, over a conventional and public communication channel the basis x or y (eigenstate of σ_x or σ_y) in which each quantum system was prepared. When the receiver has used the same basis as the emitter for his measurement, he knows that the bit value he has measured must be the one which was sent over by the emitter. He indicates publicly for which quantum systems this condition is fulfilled. Measurements for which the wrong basis was used are simply discarded. In the absence of a spy, the sequence of bits shared is error free. Although a spy who wants to get some information about the sequence of bits that is being exchanged can choose between several attacks, the laws of quantum physics guarantee that he will not be able to do so without introducing a noticeable perturbation in the key.

Other protocols – like the Bennett 92 (B92) [3] – have been proposed.

In practice, the apparatuses are imperfect and also introduce some errors in the bit sequence. In order to still allow the production of a secret key, the basis reconciliation part of the protocol is complemented by other steps. This whole procedure is called key distillation. The emitter and the receiver check the perturbation level, also know as quantum bit error rate (QBER), on a sample of the bit sequence in order to assess the secrecy of the transmission. In principle, errors should be encountered only in the presence of an eavesdropper. In practice however, because of the imperfections of the apparatus, a non-zero error probability can also always be observed. Provided this probability is not too large, it does not prevent the distillation of a secure key. These errors can indeed be corrected, before the two parties apply a so called privacy amplification algorithm that will reduce the information quantity of the spy to an arbitrarily small level.

In the last years, several demonstrations of QC systems have been implemented using photons as the information carriers and optical fibers as quantum channels. While the original proposal called for the use of single photons as elementary quantum systems to encode the key, their generation is difficult and good single-photon sources do not exist yet. Instead, most implementations have relied on the exchange between the emitter and the receiver of weak coherent states, such as weak laser pulses, as approximations to ideal elementary quantum systems. Each pulse is a priori in a coherent state $|\mu e^{i\theta}\rangle$ of weak intensity (typically the average photon number per pulse $\mu \approx 0.1$ photons). However since the phase reference of the emitter is not available to the receiver or the spy, they see a mixed state, which can be re-written as a mixture of Fock states, $\sum_n p_n |n\rangle\langle n|$, where the number n of photons is distributed according to Poissonian statistics with mean μ and $p_n = e^{-\mu}\mu^n / n!$. QC with weak pulses can be re-interpreted as follows: a fraction p_1 of the pulses sent by the emitter contain exactly one photon, a fraction p_2 two photons, and so on, while a fraction p_0 of the pulses are simply empty and do not contribute to the key transmission. Consequently, in QC apparatuses employing weak pulses, a rather important fraction of the non-empty pulses actually contain more than one photon. The spy is then not limited any longer by the no-cloning theorem. He can simply keep some of the photons while letting the others go to the

receiver. Such an attack is called photon-number splitting (PNS) attack. If we assume that the only constraints limiting the technological power of the spy are the laws of physics, the following attack is in principle possible: (1) for each pulse, the spy counts the number of photons, using a photon number quantum non-demolition measurement; (2) he blocks the single photon pulses, while keeping one photon of the multi-photon pulses in a quantum memory and forwarding the remaining photons to the receiver using a perfectly transparent quantum channel; (3) he waits until the emitter and the receiver publicly reveal the bases used, and correspondingly measures the photons stored in his quantum memory: he must discriminate between two orthogonal states, and this can be done deterministically. In this way, he obtains full information on the key, which implies that no procedure allows to distillate a secret key for the legitimate users. In addition, the spy does not introduce any discrepancies in the bit sequences of the emitter and the receiver. The only constraint on PNS attacks is that the presence of the spy should remain undetected. In particular, he must ensure that the rate of photons received by the receiver is not modified.

In the absence of the spy, the raw rate of photons that reach the receiver is given by:

$$R_{Receiver}(\delta) = \mu \cdot 10^{-\delta/10} \text{ [photons/pulse]} \quad (1)$$

where $\delta = \alpha L$ is the total attenuation in dB of the quantum channel of length L. Thus, the PNS attack can be performed on all passing pulses only when $\delta \geq \delta_c$ with $R_{Receiver}(\delta_c) \cong p_2$: the losses that the receiver expects because of the fiber attenuation are equal to those introduced by the action of the spy storing and blocking photons. For shorter distances, the spy sends a fraction q of the pulses on her perfectly transparent channel without doing anything and performs the PNS attack on the remaining 1-q fraction of the pulses. The receiver measures a raw detection rate

$$R_{Receiver|Spy}(q) = q\mu + (1-q)B \text{ [photons/pulse]} \quad (2)$$

where $B = \sum_{n\geq 2} p_n (n-1)$. The parameter q is chosen so that $R_{Receiver|Spy}(q)=R_{Receiver}(\delta)$. The information the spy gets on a bit sent by the emitter is 0 when he does nothing, and

1 when he perform the PNS attack, provided of course that the receiver has received at least one photon:

$$I_{Spy}(q) = \frac{(1-q)S}{q+(1-q)S} \text{ [bits/pulse]} \quad (3)$$

with $S = \sum_{n\geq 2} p_n$. The critical length of the quantum channel is determined by the condition $R_{Receiver}(\delta_c) = R_{Receiver|Spy}$ (q=0). For an average photon number μ =0.1, one finds δ_c= 13 [dB], which corresponds to a distance of the order of 50 km (α = 0.25 [dB/km])

Although the PNS attacks are far beyond today's technology, their consequences on the security of a QC system relying on weak coherent states is devastating, when they are included in the security analysis [4]. The extreme vulnerability of the BB84 protocol to PNS attacks is due to the fact that whenever the spy can keep one photon, he gets all the information, since he has to discriminate between two eigenstates of a known Hermitian operator, which is allowed by the laws of quantum physics.

SUMMARY OF THE INVENTION

The primary object of the invention is to allow to exchange a key featuring absolute security with a quantum cryptography apparatus using approximations, such as weak coherent states, to ideal elementary quantum systems.

It covers a new class of protocols for QC in which the emitter encodes each bit onto a pair of non-orthogonal states belonging to at least two suitable sets, which allow to neutralize PNS attacks, and lead thus to a secure implementations of QC with weak coherent states over longer distances than present protocols.

The apparatus of the emitter (see Fig. 1) consists of a source of quantum states and a preparation device. Both of these elements are controlled by a processing unit. A random number generator is connected to this processing unit, in order to allow random preparation of the quantum states. After preparation, these states are sent along a quantum channel to the receiver. The receiver consists of an analysis device followed

by a detection unit, both controlled by a processing unit. A random number generator allows the processing unit to randomly choose the analysis basis. The emitter and the receiver are connected by a conventional communication channel.

The emitter encodes each bit in the state of an elementary quantum system, belonging to either of the two sets $A = \{|0_a\rangle, |1_a\rangle\}$ or $B = \{|0_b\rangle, |1_b\rangle\}$, chosen such that $|\langle 0_a|1_a\rangle| = \eta_a \neq 0$, $|\langle 0_b|1_b\rangle| = \eta_b \neq 0$, and that there does not exist a single quantum operation, whether probabilistic or not, reducing simultaneously the overlaps of the states within all the sets (see Fig. 2, left).

In order to obtain correlated results with those of the emitter, the receiver has to distinguish between two non orthogonal states. He can do so by implementing in his analysis device a generalized measurement that unambiguously discriminates between these two states at the expense of sometime getting an inconclusive result. Such a measurement can be realized by a selective filtering, whose effect is not the same on all states, followed by a von Neumann measurement on the states that pass the filter. In the example of Fig. 2, this filter, discriminating between the elements of A, is given by $F_A = \frac{1}{\sqrt{1+\eta}}\left(|+x\rangle\langle 1_a^{\perp}| + |-x\rangle\langle 0_a^{\perp}|\right)$, where $|\psi^{\perp}\rangle$ is the state orthogonal to $|\psi\rangle$. A fraction 1-η of the states of set A passes this filter. For the states that do, the von Neumann measurement of σ_x allows their discrimination. The emitter randomly applies on each quantum system one of the two filters F_A or F_B, and measures σ_x on the outcome. Subsequently, the emitter discloses for each bit to which set A or B the associated quantum system belonged. The receiver then discards all the items in which he has chosen the wrong filter and informs the emitter.

One particular example of a protocol that belongs to this new class amounts to a simple modification of the key distillation procedure applied to bits produced by an apparatus normally used with the BB84 protocol.

The emitter sends randomly one of the four states $|\pm x\rangle$ or $|\pm y\rangle$. He applies the

convention that $|\pm x\rangle$ code for 0 and $|\pm y\rangle$ code for 1. For a given state, the receiver measures randomly σ_x or σ_y, which constitutes the most effective unambiguous way to discriminate between these states. After the exchange of a sufficiently large number of states, the emitter announces publicly one of the four pairs of non-orthogonal states $A_{\omega,\omega'} = \{|\omega_x\rangle, |\omega'_y\rangle\}$, with $\omega,\omega' \in \{+,-\}$. Within each set, the overlap of the two states is $\eta = \frac{1}{\sqrt{2}}$.

Let us assume for example that a $|+x\rangle$ was sent by the emitter, and that he subsequently announced the set $A_{+,+}$. If the receiver has measured σ_x, which happens with 50% probability, he obtains with certainty the result +1. However, since this outcome is possible for both states in the disclosed set $A_{+,+}$, it must be discarded. If the receiver has measured σ_y and obtained +1, again he cannot decide which state was sent by the emitter. However if he has measured σ_y and obtained -1, then he knows that the emitter must have sent $|+x\rangle$ and adds a 0 to his key.

The other steps of key distillation (QBER estimate, error correction and privacy amplification) remain unchanged.

Other objects and advantages of the present invention will become apparent from the following descriptions, taken in connection with the accompanying drawings, wherein, by way of illustration and example, an embodiment of the present invention is disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 schematically illustrates one embodiment of the invention, and

Fig. 2 shows an example of two sets of non-orthogonal states used in the new class of QC protocols, the four states lying in a plane of the Poincaré sphere passing through its center. Effect of the filter F_A.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Detailed descriptions of the preferred embodiment are provided herein. It is to be understood, however, that the present invention may be embodied in various forms. Therefore, specific details disclosed herein are not to be interpreted as limiting, but rather as a basis for the claims and as a representative basis for teaching one skilled in the art to employ the present invention in virtually any appropriately detailed system, structure or manner.

Referring to Fig. 1, one embodiment of the invention comprises an emitter 10 and a receiver 40 connected by a quantum channel 20 and a conventional channel 30. The emitter consists of a quantum state source 11 and a preparation device 12 controlled by a processing unit 13. A random number generator 14 is connected to the processing unit 13. The receiver 40 consists of an analysis device 41 and a detection unit 42 controlled by a processing unit 43. A random number generator 44 is connected to the processing unit 43.

The emitter generates a quantum state using his source 11 and encodes, using the preparation device 12, the value of each bit on this quantum state belonging to either of the two sets $\mathrm{A} = \{|0_a\rangle, |1_a\rangle\}$ or $\mathrm{B} = \{|0_b\rangle, |1_b\rangle\}$, chosen such that $|\langle 0_a|1_a\rangle| = \eta_a \neq 0$, $|\langle 0_b|1_b\rangle| = \eta_b \neq 0$, and that there does not exist a single quantum operation, whether probabilistic or not, reducing simultaneously the overlaps of the states within all the sets (see Fig. 2, left). The states are then sent to the receiver on the quantum channel 20.

The receiver uses his analysis device 41 to perform a generalized measurement that unambiguously discriminates between these two states at the expense of sometime getting an inconclusive result. Such a measurement is realized by a selective filtering, whose effect is not the same on all states, followed by a von Neumann measurement on the states that pass the filter. An example of such a filter, discriminating between the elements of A is given by $F_A = \frac{1}{\sqrt{1+\eta}}\left(|+x\rangle\langle 1_a^{\perp}| + |-x\rangle\langle 0_a^{\perp}|\right)$, where $|\psi^{\perp}\rangle$ is the state orthogonal to $|\psi\rangle$. A fraction 1-η of the states of set A passes this filter. For the states

that do, the von Neumann measurement of σ_x allows their discrimination. The detection unit 42 records the outcome of the generalized measurement. The processing unit of the emitter 43 randomly applies on each qubit one of the two filters F_A or F_B, and measures σ_x on the outcome. Subsequently, the emitter discloses for each bit the set A or B. The receiver then discards all the items in which he has chosen the wrong filter and informs the emitter through messages on the conventional channel 30.

The emitter and the receiver follow then the procedure of key distillation comprising the steps of QBER estimate, error correction and privacy amplification.

This new class of protocols is straightforwardly generalized to the use of quantum systems comprising more than two levels.

It can also be generalized to the cases where more than two sets of states are used.

While the invention has been described in connection with a preferred embodiment, it is not intended to limit the scope of the invention to the particular form set forth, but on the contrary, it is intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.

REFERENCES

[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, "Quantum Cryptography", Rev. of Mod. Phys. 74, (2002).

[2] Charles Bennett and Gilles Brassard, in Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175-179.

[3] Charles Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[4] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders, Phys. Rev. Lett. 85, 1330 (2000).